UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

FILED
JAN 26 2024
PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY BG DEP CLK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1840 Henry Mizelle Road, Williamston, NC 27892

Case No. 4:24-mj-1010-RJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

1840 Henry Mizelle Road, Williamston, North Carolina 27892 as further described in Attachment A.

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BRADLEY D BAKER Digitally signed by BRADLEY D BAKER Date: 2024.01.23 10:51:42 -05'00'

Applicant's signature

Bradley Baker, Special Agent - H.S.I.

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: January 26 2024

Judge's signature

City and state: Wilmington NC

Robert B. Jones, Jr, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF EASTERN DISTRICT OF NORTH CAROLINA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF THE RESIDENCE, OUTBUILDINGS, AND APPURTENANCES LOCATED AT 1840 HENRY MIZELLE ROAD, WILLIAMSTON, NC 27892	Case No. 4:24-mj-1010-RJ

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Bradley Baker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am investigating the trafficking of child pornography also known as child sexual abuse material (CSAM) via an online messaging application.

2. I am a Special Agent with the United States Department of Homeland Security (DHS), Homeland Security Investigations (HSI) assigned to the Office of the Resident Agent in Charge, Raleigh, North Carolina. I have been a Special Agent with HSI since July 2018. I am a sworn federal law enforcement officer and have authority to investigate federal offenses

pursuant to Title 18 of the United States Code. I currently conduct investigations of crimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8).

3. I am a graduate of the Criminal Investigator Training Program and the HSI Special Agent Academy at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. During the HSI Special Agent Academy, I received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs and participation in the execution of search warrants involving child pornography and seizures of computers and other storage media. I have also successfully completed the Internet Crimes Against Children (ICAC) BitTorrent Investigations, eMule Investigations, and Freenet Investigations courses held by the National Criminal Justice Training Center. I currently hold a CompTia A+ certification and have completed the Treasury Computer

Forensic Training Program for Basic Computer Evidence Recovery Training (BCERT) and Basic Mobile Device Forensics (BMDF). My past law enforcement experience includes eight years as a Special Agent with the North Carolina Alcohol Law Enforcement Division, and I hold a Bachelor of Science degree in Criminal Justice from Appalachian State University.

4. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. This affidavit is made in support of an application for a search warrant to search the location described in Attachment A, the premises located at 1840 Henry Mizelle Road, Williamston, North Carolina, 27892 (hereinafter, the "SUBJECT PREMISES"), and to search and seize contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B of this Affidavit.

6. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; communications with others who have personal knowledge of the events and

circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation to believe that contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A are located at the SUBJECT PREMISES within Martin County in the Eastern District of North Carolina.

7. The application for a search warrant, which this affidavit is offered in support thereof, is being applied for to seize contraband, instrumentalities, fruits and evidence, more particularly described in Attachment B, of violations of 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography and access with intent to view child pornography, and violations of 18 U.S.C. § 2252A(a)(2)(A), which makes it a crime to receive and distribute child pornography.

8. In summary, this Affidavit sets forth facts establishing probable cause to believe that within the SUBJECT PREMISES there is contraband, instrumentalities, fruits, and evidence of a subject who received, distributed,

accessed with intent to view, and/or possessed via the Internet, images depicting minors engaging in sexually explicit conduct.

RELEVANT STATUTES

9. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. Title 18, U.S.C. § 2252A(a)(2)(A), prohibits the knowing receipt or distribution of (a) any child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (b) any material that contains child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. Title 18, U.S.C. § 2252A(a)(5)(B), prohibits knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b)

bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. *See* 18 U.S.C. § 2256(2)(A).

f. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device. *See* 18 U.S.C. § 1030(e)(1).

g. "Storage medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

h. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral

storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

i. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the

subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

l. "Internet Protocol Address" or "IP Address" is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

m. The "Secure Hash Algorithm" (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. SHA1 is the most widely used of the existing SHA hash functions and is employed in several widely used applications and protocols. A file processed by this SHA1

operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

n. The term "GUID," as used herein, refers to the Globally Unique Identifier (GUID) identification number that may be issued by the Peer-to-Peer (P2P) software to computers offering to share files on the P2P network. A GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

o. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol

address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level read backwards—from right to left—further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

p. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website

was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

q. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

s. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on

the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices, portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

BACKGROUND REGARDING THE INTERNET/COMPUTERS AND CHILD PORNOGRAPHY

11. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately 1997. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

12. Computers and the Internet have revolutionized crimes involving child pornography. Computers serve multiple functions in connection with child pornography crimes including: a means of viewing, producing, distributing, receiving, and storing child pornography and a means of communicating with other offenders and enticing victims.

13. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone

has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

14. Today, many computers manufactured for personal use come equipped with a camera enabling the user to produce images and videos. Thus, using computers, child pornographers are readily able to produce, or request that minor victims create child pornography. Further, images and

videos created using digital cameras can easily be transferred directly to a computer. Using a scanner, computers can convert traditional non-digital photographic images into a digital format thereby enabling the digitalization of child pornography produced using a film camera.

15. Individuals interested in the sexual exploitation of children may also use technology to target minors, interact with minors, and entice minors to produce child pornography. This is often accomplished using social networking applications including but not limited to Facebook, Instagram, Kik Messenger, Discord, and Telegram.

16. The ability of computers and electronic storage media to store large amounts of digital files makes them ideal repositories for child pornography. The capacity of these devices to store digital information has grown tremendously within the last several years enabling the storage of thousands of images and videos at very high resolutions.

17. A modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Through the Internet, a computer user can contact literally millions of other users around the world. The Internet affords collectors of child pornography multiple methods for storing, obtaining, distributing, and/or viewing child pornography in a

relatively secure and anonymous fashion. These methods include, but are not limited to, email, instant messaging services, websites, social media applications, cloud storage services, message boards, and peer-to-peer file sharing networks (P2P). These same means enable those involved with child pornography to communicate with like-minded offenders and minor victims. Even in cases where cloud storage is used, evidence of child pornography can be found on the user's computer or external media in most cases.

18. Mobile devices, hand-held computers, can transfer media through multiple methods—cellular signal, Wi-Fi, Bluetooth, and near field communication (NFC). In addition, mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with cloud storage and paired devices. For example, an individual using Google Pictures or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or "synced," with their other computer devices.

19. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, application data, temporary files, or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

20. Individuals involved in the receipt, possession, access with intent to view, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that can connect to the internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are

often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction, and prior versions can often be used until the current device is repaired or replaced.

21. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser

typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATION

22. This warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers were used, the purpose of their use, and who used them.

23. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found on the devices and/or digital storage media, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user generated. Some of these electronic records, as explained below, might take a form that becomes

meaningful only upon forensic analysis. In addition to user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records, as described further in the attachments. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from computer usage during relevant times.

24. Because the absence of particular data on a digital device may provide evidence of how a digital device has been used, what it has been used for, and who has used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.

25. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge, and intent. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

PROBABLE CAUSE

26. On October 20, 2023, a Homeland Security Investigations (HSI) Special Agent (SA) acting in an undercover capacity (UCA_1) observed the user "lollip0p11" (LOLLIP0P11) upload and share three pictures of child sexual abuse material (CSAM) within an online public group messaging application.[1] I reviewed these files and determined they clearly contain child pornography:

> File Name: Unknown
> Uploaded: October 20, 2023, at 11:16 p.m. Eastern Daylight Time (EDT)
> This picture shows a completely nude prepubescent female child laying on her back. An adult male is seen inserting his penis into the child's anus.
>
> File Name: pthc-after-fuck.jpg
> Uploaded: October 20, 2023, at 11:18 p.m. EDT
> This picture depicts a prepubescent female child laying on her back and is nude from the waist down. The female child has her legs spread apart exposing her vagina to the camera. A substance that appears to be semen is observed running out of her vagina.
>
> File Name: session-2023-02-27-214423.jpg
> Uploaded: October 20, 2023, at 11:19 p.m. EDT
> This picture shows a completely nude prepubescent female child laying on her back on what appears to be a couch. The child's legs are spread apart exposing her vagina to the camera.

1 The name of this online messaging application is known to the affiant but is being withheld to protect other ongoing investigations within this messaging platform.

27. Between the dates of October 23, 2023, and November 9, 2023, UCA_1 and LOLLIP0P11 engaged in direct communication with each other within the messaging application. At the beginning of the conversation, UCA_1 portrayed themselves as a parent who is open to other adults having sexual contact with their four-year-old daughter. During the conversations, LOLLIP0P11 revealed he is a 26-year-old male, lives near Greenville, North Carolina, his name is Austin, he is six feet tall, weighs 160 pounds, has one tattoo of a quote on his wrist, and his zodiac sign is "cancer". This conversation centered around attempting to coordinate a meeting for the purpose of LOLLIP0P11 having a sexual encounter with UCA_1's four-year-old daughter.

28. Within the messaging application, when asked what ages he is into, LOLLIP0P11 responded, "5-15 but I dont mind lower". When UCA_1 informed she has a four-year-old daughter with no experience, LOLLIP0P11 stated, "I don't mind 4 yr olds". Also, during the chat, LOLLIP0P11 told UCA_1 he had a previous sexual encounter with his niece who is a minor.

29. LOLLIP0P11 stated, "I bought a new toy to maybe help prepare me for when that day comes haha. Of course not first thing, but later if you are cool with me". LOLLIP0P11 sent UCA_1 a picture of a hand holding a

small sex toy with two small holes in it, and later responded, "Both are super tight. Barely can't fit the top". When UCA_1 asked LOLLIP0P11 what the toy helps him do, he responded, "Just help imagine how tight it would be".

30. On November 7, 2023, LOLLIP0P11 provided UCA_1 with the Snapchat moniker, "austinuptown0" (AUSTINUPTOWN0) and requested to communicate with UCA_1 on Snapchat.

31. On November 13, 2023, UCA_1 and AUSTINUPTOWN0 began communicating with each other on the Snapchat platform. AUSTINUPTOWN0 sent what is believed to be a selfie picture of himself to UCA_1. The picture shows a young adult male with a beard and a caption of "Heya". During the Snapchat conversation, UCA_1 and AUSTINUPTOWN0 continue talking about UCA_1's four-year-old daughter and possibly coordinating a meeting.

32. AUSTINUPTOWN0 sent UCA_1 a picture of a small sex toy with two small holes in it with a caption of "Might get ready to use this". This sex toy appears to be the same toy sent previously to UCA_1 from LOLLIP0P11 on the messaging application.

33. A Department of Homeland Security summons was served on Snap, Inc., for the subscriber information associated with the account:

austinuptown0. As a result of the summons, Snap, Inc., provided the following account information:

Display Name: Austin Evens
Date Creation: November 5, 2023
Creation IP Address: 172.59.217.143
Verified Phone Number: (252) 327-2246
Last Recorded IP Address: 74.196.89.23 on December 7, 2023
Other Account IP Activity: 74.196.89.23 on November 7 and 13, 2023

34. A query was made on the IP address 74.196.89.23 through the American Registry for Internet Numbers (ARIN). ARIN reported IP address 74.196.89.23 to be registered to Suddenlink Communications which is now Optimum.

35. A Department of Homeland Security summons was served on Optimum for the subscriber utilizing the IP address 74.196.89.23 for the date of November 7, 2023. As a result of the summons, Optimum provided the following account information:

Subscriber: James Chambers
Service Address: 1840 Henry Mizelle R, Williamston, NC 27892
Telephone Number: 252-809-3085
Email Address: jcham89@suddenlink.net

36. IP Logs detailed the subscriber was assigned the IP address of 74.196.89.23 between the dates of September 13, 2023, and November 21,

2023. Logs showed the subscriber was previously assigned the IP address of 74.196.89.229.

37. A query conducted through the North Carolina Department of Motor Vehicles revealed that Alexander Madison CHAMBERS with a date of birth of XX/XX/1998 was issued a NC Driver's License listing the SUBJECT PREMISES as his address. The image associated with the Driver's License bears a close resemblance to the images of the adult male received by UCA_1 from AUSTINUPTOWN0. Based on the birthdate listed on CHAMBERS' driver's license his zodiac sign would be "Cancer". CHAMBERS' license also lists him as six feet tall.

38. I conducted an open-source search of the Facebook platform. I located a profile with the name of "Alex Chambers". The profile states the individual lives in Williamston, North Carolina. The profile picture as well as other pictures posted in this account clearly matches the person in the pictures sent to UCA_1 from AUSTINUPTOWN0. In one picture on the account, a tattoo, "VENI VIDI VICI", can be seen on the inside of the individual's right wrist.

39. Pictures found within the Facebook account show a black Dodge Charger bearing North Carolina registration plate of "ELLI57". A search of

the NC Department of Motor Vehicles shows this vehicle is registered to CHAMBERS at the SUBJECT PREMISES. I also located a picture in the Facebook account depicting a female child. The picture contains a caption written by "Alex Chambers" that states, "She takes after her uncle alex...".

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

40. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law

enforcement officers involved in the investigation of child pornography throughout the world.

BIOMETRIC ACCESS TO DEVICES

41. This warrant permits law enforcement to compel Alexander CHAMBERS to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a

device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises.

For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search.

The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the

event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Alexander CHAMBERS to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of Alexander CHAMBERS and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of Alexander CHAMBERS and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Alexander CHAMBERS state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel

Alexander CHAMBERS to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

42. As described in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the search and seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. *Probable cause.* I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium,

deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data

structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging

systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times

and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other

evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context,

draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

45. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic

evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

47. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

48. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of offenses in violation of 18 U.S.C. § 2252A, as more fully described in Attachment B of this Affidavit, may be located at the residence described in Attachment A.

49. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES and the search and seizure of the items listed in Attachment B to include a full forensic examination of any computers, electronics, and related devices listed here.

BRADLEY D BAKER
Digitally signed by BRADLEY D BAKER
Date: 2024.01.24 08:58:38 -05'00'

Bradley Baker
Special Agent
Homeland Security Investigations

Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3), this 26 day of January 2024.

Robert B. Jones, Jr
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The entire property located at 1840 Henry Mizelle Road, Williamston, NC 27892, including the residence, any outbuildings, and other structures on the premises, and any appurtenances thereto (all which constitute the SUBJECT PREMISES). The residence is described as a two-story single-family home. The house is made of red brink on the front with a covered porch spanning the entire length. A white garage door can be seen on the left side of the front of the house. A gravel "U" shaped driveway intersects Henry Mizelle Road on the left and right side of the residence and extends around the backside of the house. A black mailbox is placed at the end of the driveway. Below the mailbox a green sign displays the number "1840". See photograph below:

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);
    b. records and information referencing child erotica;

c. records, information, and items referencing or revealing the occupancy or ownership of 1840 Henry Mizelle Road, Williamston, NC 27892 including utility and telephone bills, mail envelopes, or addressed correspondence;

d. records and information referencing or revealing the use of peer-to-peer software, including BitTorrent client software;

e. records and information revealing sexual interest in minors;

f. records and information referencing or revealing trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

g. records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

h. records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography; and

i. records and information revealing the use and identification of remote computing services such as email accounts or cloud storage.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER;

i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child sexual exploitation content.

7. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

8. During the execution of the search of the PREMISES described in Attachment A law enforcement personnel are also specifically authorized to compel Alexander CHAMBERS to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

9. This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any

DEVICE. Further, this warrant does not authorize law enforcement personnel to compel that Alexander CHAMBERS state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives,

flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.